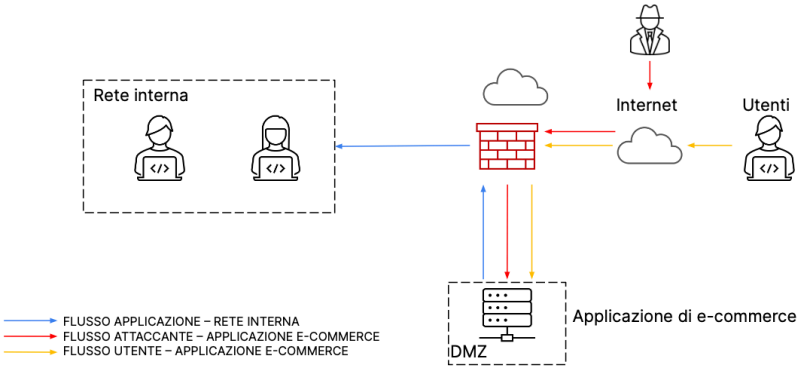
5. Analisi dei log – caso reale

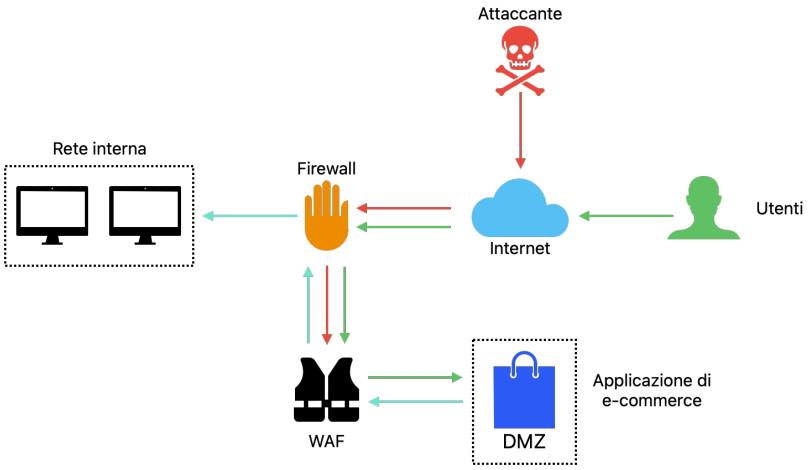
Con riferimento alla figura sottostante, rispondere ai quesiti.



L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.
La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.

Azioni preventive

Implementazioni azioni di prevenzione per la difesa dell'applicazione Web da attacchi di tipo SQLi o XSS



Azioni di prevenzione a livello Web

- Verificare e validare i dati di input degli utenti.
- Utilizzare i parametri nelle query SQL per evitare l'iniezione di codice.
- Verificare che i dati inseriti dagli utenti siano conformi a specifici criteri. In questo modo, gli utenti non saranno in grado di inserire codice malevolo come parte dei dati di input.
- Utilizzare librerie di sicurezza specifiche per la gestione delle vulnerabilità XSS e SQLi.
- Configurare correttamente il server web per limitare l'accesso ai file e alle cartelle sensibili.
- Formare il personale sulla sicurezza delle applicazioni web e sui rischi associati alle vulnerabilità XSS e SQLi, per ridurre al minimo le possibilità di errore umano.
- Monitorare costantemente l'applicazione web per individuare eventuali attacchi.

Azioni di prevenzione a livello di rete.

- Utilizzo di dispositivi di sicurezza dedicati (WAF)
- Limitare l'accesso alla DMZ solo ai servizi che devono essere esposti all'esterno e solo ai clienti autorizzati.

- Monitorare costantemente il traffico in ingresso e in uscita della DMZ per individuare eventuali attacchi o anomalie.
- Mantenere i server e le applicazioni nella DMZ aggiornati con le ultime patch di sicurezza.
- Eseguire backup regolari dei dati nella DMZ per garantire che i dati siano al sicuro.
- Eseguire test di sicurezza regolari sulla DMZ per individuare eventuali vulnerabilità.
- Formare il personale che gestisce la DMZ sulla sicurezza delle reti e sui rischi associati.

Impatti sul business

L'applicazione Web subisce un attacco di tipo DDoS

Applicazione **non raggiungibile per 10 minuti**.
Calcolando che l'impatto sul business, alla non raggiungibilità del servizio, è di 1.500 euro ogni minuto, **il danno subito è di 15.000 euro.**

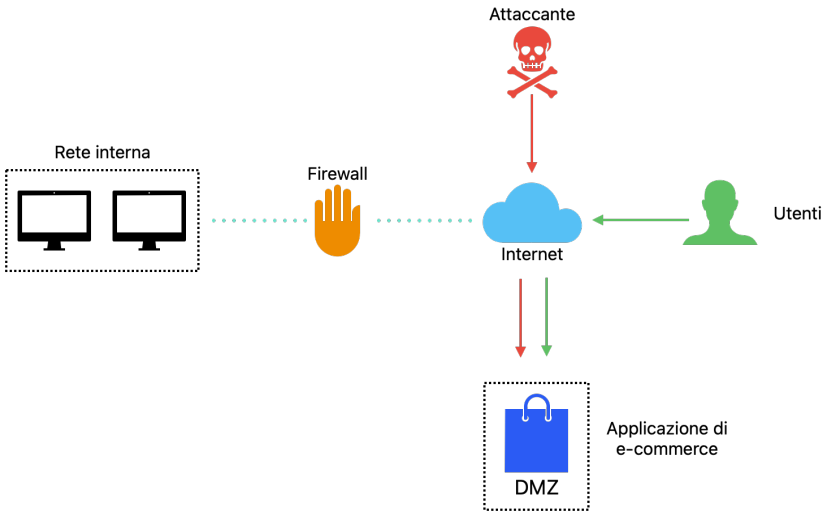
Valutazioni di azioni preventive che si possono adottare.

- Utilizzare un firewall DDoS può aiutare a rilevare e mitigare gli attacchi DDoS in tempo reale.
- Utilizzare un servizio di mitigazione DDoS che sono in grado di rilevare e bloccare gli attacchi DDoS.
- Ridurre la superficie di attacco delle web app limitando l'accesso solo ai servizi necessari e utilizzando una buona architettura di sicurezza.
- Effettuare test di sicurezza regolari per individuare eventuali vulnerabilità nelle web app.
- Pianificare la continuità del servizio in caso di un attacco DDoS, ad esempio utilizzando server di backup o servizi di ridondanza.
- Aggiornare regolarmente i software.
- Monitorare costantemente il traffico in ingresso e in uscita delle web app.

Response

L'applicazione Web viene infettata da un malware

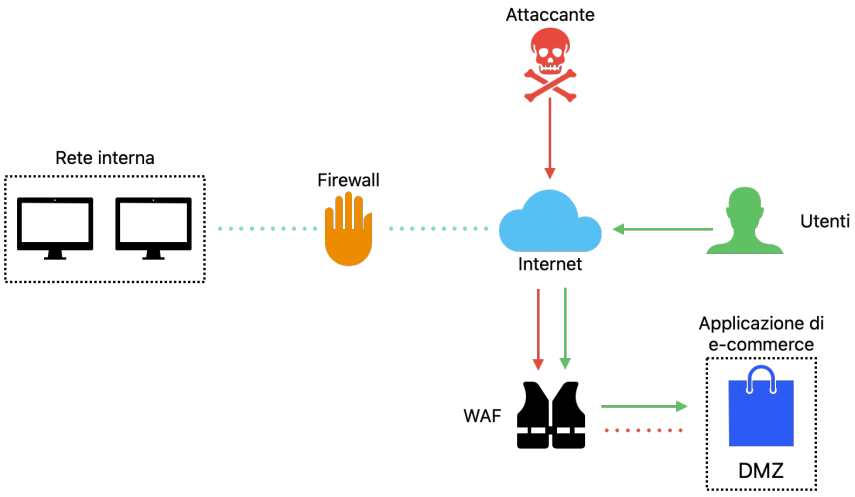
Priorità nel non far diffondere il **malware** sulla nostra rete.
Ci viene richiesto inoltre di non interessarci a rimuovere l'accesso dell'attaccante dalla macchina infetta, pertanto lo schema che andremo a modificare, risulterà in questo modo:



In questo modo riesco ad **isolare** l'applicazione dalla nostra rete interna per evitarne una diffusione del malware.

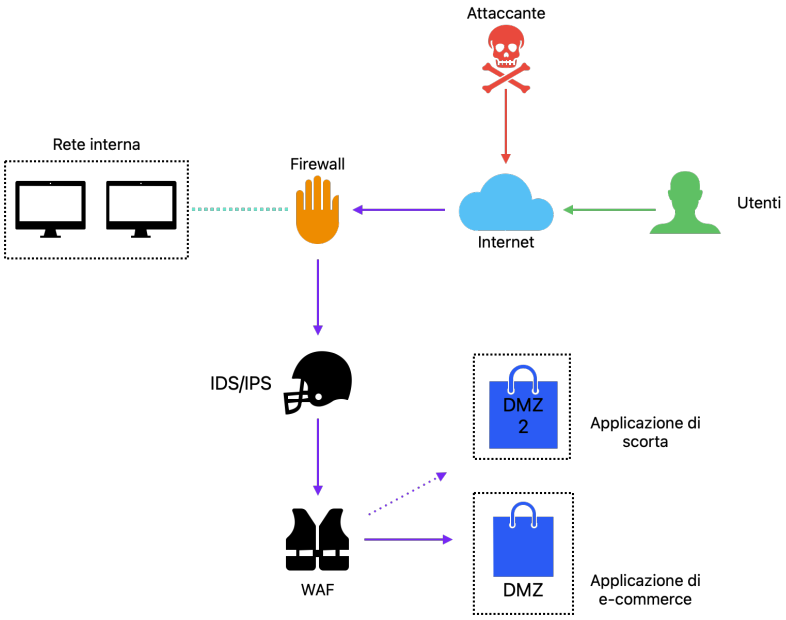
Soluzione completa

Unione dell'azione preventiva e della response



In questo modo, con l'unione, l'attaccante potrà comunque avere accesso all'applicazione, ma attraverso il WAF non riuscirà a sfruttare l'SQLi e l'XSS.

Modifica più aggressiva dell'infrastruttura



In questo caso implementiamo **configurazioni** specifiche del **firewall**, aggiungiamo un sistema di rilevamento delle intrusioni **(IDS/IPS)** ed un dispositivo di sicurezza per applicazioni Web **(WAF)**. Inoltre possiamo andare a creare una seconda **DMZ (di scorta)** in caso di problemi con la prima DMZ, dovuta ad una compromissione, per garantire la sicurezza della rete interna. La creazione di una seconda DMZ comporta un costo maggiore da sostenere per l'azienda.